USDA COMPUTER INCIDENT RESPONSE PROCEDURES MANUAL

TABLE OF CONTENTS

Page

TABLE OF CONTENTS

CHAPTER 1 – GENERAL INFORMATION

1	Purpose	1
2	Cancellation	1
3	Scope	1
4	Abbreviations	2
5	Definitions	2

Part I - Computer Incident Response Procedures

1	Background	6
2	Policy	7
	Incident Reporting Process	7
	Assessment & Containment	10
	Recovery Operations	11
	Damage Analysis and Determination	11
	Law Enforcement Responsibilities	12
	Incident Response Forms & Time Frames	12
	Process for Invoking Cyber Corps	13
3	Responsibilities	14

FIGURES

Daily Incident Report	25
IT Incident Report	26
OCIO Incident Contact List	31
Agency Incident Contact List	32
IT Incident Process Chart	33

DEPARTMENTAL MANUAL

SUBJECT:	DATE: 10/25/01
USDA Computer Incident Response Procedures	OPI: OCIO, Cyber Security

CHAPTER 1

GENERAL INFORMATION

1 PURPOSE

This Departmental Manual establishes policy and procedures for reporting Major Information Technology (IT) incidents that may compromise the availability, integrity, and confidentiality of Department of Agriculture (USDA) IT and telecommunications resources. The purpose of an incident reporting policy is to facilitate cooperation and information exchange among all USDA personnel who have responsibility for detection, reporting and notification of security incidents to management and legal authorities. This manual is issued to augment the following laws, regulations, directives: the Computer Security Act of 1987; National Institute of Standards and Technology Special Publication 800-3, and Office of Management and Budget Circular A-130, Appendix III.

2 SPECIAL INSTRUCTIONS/CANCELLATION

This Departmental Manual replaces:

a OCIO Memorandum Final Agency Review Computer Incident Reporting Procedure dated 3/8/99;
b OCIO memorandum Incident Response Coverage, dated 6/29/99;
c OCIO memorandum Incident Response Coordination Center, dated 7/2/99.
d This chapter replaces Incident Reporting Procedures in DM 3140, ADP Security Manual and DR 3140-001 ADP Security Policy.
e This manual will be in effect until superseded.

3 SCOPE

This manual identifies the USDA's procedures for promptly reporting intrusions into Information Technology (IT) systems and establishes formal reporting requirements for all such instances to the USDA Chief Information Officer (CIO). All security incident reports are to contain the facts and

information needed to make informed management decisions and to assist in managing the resolution(s). This regulation applies to all USDA agencies, programs, teams, organizations, contractors, consultants, appointees, employees of USDA funded councils, associations, other government agencies and state/local governments and committees that use, process, manage USDA information or meet the requirements of "operator of a Federal computer System".

4 ABBREVIATIONS

CIO	- Chief Information Officer
CS	- Cyber Security
FBI	- Federal Bureau of Investigation
FTP	- File Transfer Protocol
I/D	- Intrusion Detection
IP	- Internet Protocol
IRT	- Incident Response Team
ISSO	- Information Systems Security Officer
ISSP	- Information Systems Security Program
ISSPM	- Information Systems Security Program Manager
IT	- Information Technology
NITC-SNCC	- National Information Technology Center – Systems Network Control Center
OCIO	- Office of the Chief Information Officer
OIG	- Office of the Inspector General
POC	- Point of Contact
OMB	- Office of Management & Budget
USDA	- United States Department of Agriculture

5 DEFINITIONS

Breach - Any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

Chain of Custody - Protection of evidence by each responsible party to ensure against loss, breakage, alteration or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence. Individuals shall place their initials and date on the container when the evidence is stored in a container or on the evidence in such a way that no damage is incurred.

Compromise – A compromise is to invade something by getting around its security. A computer has been compromised, for example, when a Trojan Horse has been installed.
Compromise of Integrity – A compromise of integrity is any unauthorized modification of the correctness of information or data.

Computer Security Incident – A computer security incident is any adverse event whereby some aspect of a computer system is threatened: loss of data confidentiality, disruption of data or system integrity, disruption or denial of availability. Some examples are listed below:

Intrusion of computer systems via the network (often referred to as "hacking");
The occurrence of computer viruses and/or resulting damage;
Unusual or suspicious probes for vulnerabilities via the network to a range of computer systems (often referred to as scans);
Unusual processes, not installed by USDA, running on server.

Within the computer security arena, these events are often simply referred to as "incidents". The definition or identification of an incident may vary for each USDA agency or mission area depending on the situation. However, the following categories (also defined in this section) are generally applicable: Compromise of Integrity, Denial of service, Misuse, Damage, and Intrusions.

Damage – Damage is the unauthorized deliberate or accidental modification, destruction or removal of information or data from a computer system.

Denial of Service – Denial of service is an inability to utilize system resources due to unavailability; for example, when an attacker has disabled a system, a network worm has saturated network bandwidth, an IP address has been flooded with external messages or "a system manager and all other users become locked out of a UNIX system, which has been changed to single user mode."

Firewall - A security policy and technology that defines the services and accesses permitted, and an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall is to restrict access to or from a protected network. It implements a network access policy by forcing connections to pass through the firewall, where they are examined and

evaluated. A USDA firewall must use stateful inspection technology that is aware of the content and state of connection. This technology, which denies all traffic unless it is specifically allowed, employs rules targeted squarely at implementing security decisions at all levels; effectively log activities; filters throughout all levels of the protocol stack; tracks valid active sessions, and processes/filters/tracks high level applications such as electronic mail, file transfer and hyper-text transmission.

Harm – Harm is to damage, injure or impair Information Technology (IT) systems using electronic methods.

Incident Handling - This refers to the actions taken to resolve the incident.

Incident Oversight – This process is the ongoing surveillance of the networks and systems to spot new vulnerabilities and take corrective actions in advance of incidents.

Incident Reporting - This involves formal acknowledgement that a computer incident occurred.

Incident Response – This process is the analysis of how the incident happened and how to handle the situation so that it does not reoccur.

Intrusion – Intrusion is an unauthorized, inappropriate or illegal activity by insiders or outsiders that can be considered a penetration of a system.

Intruder - An intruder is a person who is the perpetrator of a computer security incident. Intruders are often referred to as "hackers" or "crackers." Hackers are highly technical experts who penetrated computer systems; the term Crackers refers to the experts with the ability to "crack" computer systems and security barriers. Most of the time "cracker" is used to refer to more notorious intruders and computer criminals. An intruder is a vandal who may be operating from within USDA or attacking from the outside of Department.

Level of Consequence - The impact an incident has on an organization. Impact includes: loss of data; the cost to a USDA agency or mission area; negative consequences to the organization (e.g. damage to reputation); and the magnitude of damage that must be corrected.

Misuse - Unauthorized use of an account by an intruder (or insider)constitutes misuse.

Need-to-Know - The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially sanctioned duties. Responsibility for determining whether a person's duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not upon the prospective recipient. This principle is applicable whether the prospective recipient is an individual, a contractor, another Federal agency or a foreign government.

Threat – A threat is circumstance, condition, or event with the potential to cause harm to personnel and/or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste and abuse. The most common security threats are to network systems. Network security threats include impersonation, eavesdropping, denial of service, packet replay/modification.

CHAPTER 1 – PART 1
INCIDENT RESPONSE PROCEDURES

1 BACKGROUND

Global network connectivity is common place for information exchange and is crucial for conducting everyday operations. However, the benefits can be overshadowed by the increase in network vulnerabilities. The number of Internet related incidents that have occurred in the past year, along with the increase and complexity of threats, requires that USDA take their incident handling capability seriously. Networks and IT resources are continually vulnerable to illegal/ malicious activity or exploitation by internal and external sources. The most common security threats are to network systems. Network security threats include impersonation, eavesdropping, denial of service, packet replay/modification. Damage to IT systems from a computer security incident (intrusion) can occur in a short period. Therefore it is essential that all USDA organizations have procedures in place that can be activated immediately. The failure of an agency or mission area to promptly report an intrusion impacts and potentially compromises the Information Systems Security Program (ISSP) efforts of other USDA organizations and their customers. Section 5, General Information, contains definitions for the Incident Response terminology used in this chapter.

There is a strong need for all USDA agencies to notify the reporting hierarchy and follow all incident reporting procedures. Every attempt should be made to capture accurate information from the outset, preserve evidence, and share lessons learned on the IT Incident Report form, Figure 2 of this manual. Standard reporting and uniform operating procedures permits USDA to be better positioned for assessing risks, addressing vulnerabilities, reducing overall costs and meeting the security challenges of USDA's information infrastructure.

Figures are included in this document for agency use in incident reporting. Completed Incident Report information shall be declared to be sensitive and sharing/distribution of the information shall be limited to individuals with a valid need-to-know. The USDA CIO, Deputy CIO or the Associate CIO for Cyber Security will review requests for the release of this information and make determinations with regard to release of this information, consistent with applicable Federal Statutes. Overall

questions regarding this policy should be directed to the USDA Office of the Chief Information Officer, Cyber Security.

2 POLICY

a Incident Reporting Process. All USDA agencies and staff offices shall establish and implement an internal incident response capability. Intrusions, the focus of this Regulation, are only one form of computer security incident. A computer security incident is any adverse event whereby some aspect of a computer system is threatened: loss of data confidentiality, disruption of data integrity, disruption or denial of service. The types of incidents have been classified into low, medium or high levels depending on the severity.

Low level IT Incidents are the least severe and should be handled within one working day after the event occurs by the agency ISSPM.

These include:

- Loss of Personal Password
- Suspected Sharing of USDA Accounts
- Misuse of Computer Equipment
- Unintentional Routine Computer Actions
- Unsuccessful Scans/Probes
- Computer Virus/Worms (Depending on Impact to Agency/Department)

Medium Level IT Incidents are more serious and should be handled the same day the event occurs (normally in two to four hours of the event).

These include:

- Unfriendly Employee Termination
- Violation of Special Access
- Illegal Building Access
- Unauthorized use of a system for processing or storing USDA data
- Property Destruction related to a computer incident (less than $100,000)
- Personal Theft related to a computer incident (less than $100,000)
- Computer Virus/Worms (Depending on Impact to Agency/Department)

High Level IT Incidents are the most serious and considered "Major" in nature. Because of the gravity of the situation and the high potential for harm to USDA, these incidents should be handled as soon as possible.

These include:

- Suspected Computer Break-In
- Denial of Service Attacks
- Computer Virus/Worms (Depending on Impact to Agency/Department)
- Unauthorized use of a system for processing or storing Non-USDA or prohibited data
- Changes to system hardware, firmware or software without the system owner's authorization
- Property Destruction related to a computer incident (exceeding $100,000)
- Personal Theft related to a computer incident (exceeding $100,000)
- EFT File Exploitation/Manipulation
- Warez (Illegal Software Download/Sale)
- Child Pornography
- Pornography
- Download of Music/Unauthorized Software
- Any violation of law

High Level "Major" IT Incidents which include Warez, Child Pornography, Pornography, Downloading Music/Unauthorized Software, any violation of law or On Line Gambling will be handled using an accelerated and confidential IT Incident Response. Agency ISSPMs who have suspected events of this nature are to immediately contact and coordinate the incident response with the Associate CIO for Cyber Security/Designate in handling these events.

Other types of incidents include *isolated* viruses or misuse of computer equipment, unintentional actions, and common, unsuccessful scans or probes. When faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps protect the information of others that might be affected by the incident.

The need for an incident handling capability that crosses agency

boundaries has never been greater. An incident is the act of violating an explicit or implied security policy. The types of activity that are widely recognized as being violations of a typical security policy are characterized below. These activities include but are not limited to:

(1) attempts (either failed or successful) to gain unauthorized access to a system or its data
(2) unwanted disruption or denial of service
(3) the unauthorized use of a system for the processing or storage of data
(4) changes to system hardware, firmware or software characteristics without the owner's knowledge, instructions, and approval

The level of consequence of an incident refers to the relative impact it has on an organization. The types of impact include: loss of data; the loss of revenue or confidence in a USDA agency or mission area by the general public or customers; or a high level of damage that must be corrected prior to system restoration.

The serious nature of incidents dictates that USDA and its agencies have an effective Computer Incident Response Procedure. There are four major segments involved in an effective Computer Incident Response Procedure; they are: reporting, handling, response and oversight. Incident Reporting involves formal acknowledgement that a computer incident occurred. Incident Handling refers to the actions taken to resolve the incident. Incident Response is the analysis of how the incident happened and how to handle the situation so that it does not reoccur. Finally Incident Oversight refers to the ongoing surveillance of the networks and systems to spot new vulnerabilities and take corrective actions in advance of incidents. Figure 5, IT Incident Process chart outlines the overall incident process within USDA agency/mission areas. The goal of this procedure is to respond to each incident effectively and as close to real time as possible to protect USDA's information assets.

Each agency will develop documentation at the outset that shall be updated during each stage of the incident, and shall be finalized after the incident is closed. The CIO, through the CS, shall be kept abreast of the status of ongoing incident efforts at regular intervals (i.e., as often as events change or significant progress is made) by the agency, mission area, or ISSPM. The CIO shall notify the Secretary by Informational Memorandum about significant

breaches and provide regular updates to the Secretary, as appropriate. OCIO, in coordination with of Office of Communications, shall be responsible for all dealings with the media and with the public. USDA agency/mission area employees are instructed to direct inquiries from the public, including the news media, to OCIO. [Specific information on required actions for Incident Reporting can be found in Section 6, Responsibilities]

b Assessment & Containment. Each agency will develop internal reporting procedures that support the actions required by this policy and define the actions that must be taken in responding to and reporting security incidents. At a minimum, internal procedures will include the agency reporting chain and require the involvement of the agency personnel and Departmental ISSPM. These procedures will also require preservation of evidence, assessment, containment and recovery actions, damage determination, report documentation, lessons learned, and identification of corrective actions required by agency security programs.

Agencies and staff offices will distribute this procedure to all appropriate personnel with the responsibility for identifying, reporting, or handling of Major IT Incidents. Responsible parties shall be instructed to read and become familiar with the incident reporting policy. Agency individuals assigned to incident handling or reporting may be organized into a response team that becomes active when a breach is identified.

All USDA networks will be monitored on a daily ongoing basis. It is not necessary to procure and install I/D devices or software for every server. Only the most critical locations need to have I/D installed. As soon as suspicious activity is detected, personnel qualified and designated to respond shall be notified to take immediate action. Each Agency Management Staff must assess and be empowered to take containment actions up to and including shutting a system down within a reasonable time after discovery of an intrusion to prevent further intrusion or damage. The Associate CIO for Cyber Security/Designate will issue a "Cease and Desist" Order to bring the system down, if the agency does not respond and the problem is not contained in a timely manner (normally 12 hours). Reporting through agency channels and to the Department shall occur simultaneously when accurate information is available, particularly in cases where the preliminary assessment indicates that significant damage to USDA resources may have

occurred. Upon confirmation, the incident response actions must be implemented immediately. Unavailability of any official in the reporting chain is not to delay the continuation of the incident notification or response process. [Specific information on required actions for Assessment and Containment can be found in Section 6, Responsibilities]

c Recovery Operations. Each agency/mission area should prioritize those actions that support the smooth recovery of a compromised system(s). In no case should a compromised system, web page or application be returned to normal operation without the approval of Associate CIO for Cyber Security. The ISSPM will request that CS permit the system(s), web page, or application to resume normal operation. CS reserves the right to further scan the system to ensure that appropriate security is in place to protect the department. The agency may resume normal operation of the restored system, upon CS approval and the completion of the IT Incident Report. The CS will have 1 working day to respond with the approval/disapproval to return the system to normal operation. If a system is Mission Critical, agencies can coordinate directly with the Associate CIO for Cyber Security for a more immediate system restoration, on a case by case basis. If the agency does not receive a response within that time, they can return the system to normal operation provided that they feel adequate security protection is in place to prevent future incidents. [Specific information on required actions for Recovery Operations can be found in Section 6, Responsibilities]

d Damage Analysis and Determination. A Damage Analysis of all IT Incidents is to be initiated immediately after assessment, containment and recovery actions by each agency ISSPM. The ISSPM will determine if the incident is confined to one agency or multiple agencies and if there is impact to organizations outside USDA. The impact to each system will be analyzed to determine if the control of the system has been compromised. All compromised systems will be disconnected from external communications as soon as possible, but not later than 12 hours from discovery of the incident. Control of a system is lost when the intruder obtains control of the root or system accounts with administrative privileges. A determination is to be made if log files have been erased or compromised.

The ISSPM will initiate the process of estimating the overall economic impact of the incident to the agency/mission area and USDA in coordination with the System Owner/Business Manager. At a minimum, the estimate will be quantified in terms of loss of system(s) availability, loss of response capability to customers, cost of equipment/software to repair, and hours of personnel associated with the repair or restoration of the system(s). The damage assessment report will be reviewed and concurred by the System Owner/Business Manager prior to inclusion in the IT Incident Report. This information will then be updated in the IT incident Report, Figure 2. [Specific information on required actions for Damage Analysis and Determination can be found in Section 6, Responsibilities]

e Law Enforcement Responsibilities. The OIG regards threats using computers as "Workplace Violence. Incidents are referred to the FBI, Violent Crimes Unit. More information on Workplace Violence can be obtained from the Violence Prevention Program Website http://www.usda.gov/da/workviolence.htm.

Threats of harm to a USDA employee or contractor at the official duty station by someone using computer E-mail are a serious type of security incident. All acts of violence should be promptly reported to supervisors or managers and in the case of an emergency, directly reported to the USDA Local Security Guard Command Center. Any agency ISSPM or representative who receives a report of a threat using electronic equipment should complete a Daily Intrusion Report, Figure 1, and forward the information to CS for referral to the OIG.

IT Incidents, deemed major in nature by CS involving computer systems, websites and applications, are also reported to the OIG. The OIG will review the case (incident) and routinely advise CS of the disposition within 30 days from receipt of the official report. Possible disposition includes: internal investigation, referral to the FBI, or no action. In cases of no OIG response the Associate CIO for Cyber Security, through the CIO, can escalate cases for disposition.

The Associate CIO for Cyber Security, through the CIO, can escalate the matter to the Inspector General for accelerated support and case disposition in major IT Incidents involving a high threat magnitude. In those instances, the OIG will respond within 5 working days from receipt of the official report.

f Incident Response Forms, Contact Lists and Time Frames. Every agency/mission area must use the following Incident Reporting Forms And Contact Lists in order to properly respond to IT Incidents. Each form has time frames for required agency action.

(1) Daily Incident Report Form (Figure 1) is to be utilized to provide preliminary information to the CS for all IT Incidents by the ISSPM or Agency Representative. It is critical that this form be completed and sent to the CS within 24 hours of notification of an incident regardless of the source of the notification or level of magnitude.

(2) IT Incident Report (Figure 2) is to be used by the ISSPM or designate to update major incident information throughout the entire incident response process. The final report is to be completed not later than 30 days from official notification of each major IT Incident.

(3) OCIO Incident Contact List (Figure 3) contains the contact information to be used in responding to major IT Incidents, including contacts at National Information Technology Center – System Network Control (NITC-SNCC) and Law Enforcement activities. The purpose of this list is provide OCIO contact information to Agency Heads and other high level officials should they require it in the resolution of major IT Incidents. This is not to be used for routine inquiries made to OCIO; routine questions or concerns should be directed to CS. CS will maintain and update this list as required.

(4) Agency Incident Contact List (Figure 4) contains the agency IT Incident contact information. Each agency/mission area is responsible for providing this list to Cyber Security. CS will maintain this list electronically and provide this list to the OCIO, NITC-SNCC. NITC-SNCC will use this list in their IT Incident Notification process. This list should include the agency ISSPM and other agency representatives who are responsible for maintaining/operating agency systems/networks. All individuals identified should have the technical knowledge to support USDA's overall incident response program effectively and provide internal notification to agency officials when major IT Incidents occur. For each individual system or network, an alternate contact should be identified in order to accelerate the notification and response process. The accuracy of the names, phone

numbers and E-mail addresses is the responsibility of each agency/mission area; each ISSPM will review and update this information every 30 days. [Specific information on these forms and lists can be found in Figures 1-4]

g Process for Invoking Cyber Corps. The CS has recruited and is in the process of training a departmental incident response team referred to the "Cyber Corps" to assist agencies in IT Incident Response activities. The Cyber Corps is not intended to replace or alleviate the need for each agency to develop an internal IRT. Rather the members of this team are to be available, at the discretion of the Associate CIO for Cyber Security, in cases of serious incidents where the agency is unable to resolve the problem or if the incident represents an serious threat to the department as a whole. [Specific information on Invoking the Cyber Corps can be found in Section 6, Responsibilities]

3 RESPONSIBILITIES

a The Chief Information Officer and Deputy will:

Assessment and Containment

(1) Be notified immediately after confirmation that a security breach has occurred;
(2) Have final authority on all decisions relating to the management/response to an IT incident;
(3) Be responsible for notifying the Secretary with information concerning all Major IT Security Incidents; provide regular updates based on the gravity of the threat;

Incident Reporting

(1) In coordination with the Office of Communications, will make determinations regarding release of information consistent with applicable Federal Statutes or regulations and serve as the contact point with the media.

b The Associate Chief Information Officer for Cyber Security will:

General

(1) Function as the Department ISSO;
(2) Coordinate management of the IT Computer Incident within OCIO and external organizations, assuring that all reports and responses are prepared, appropriate personnel are involved,

appropriate organizations are contacted, and proper actions are taken to resolve the incident;

(3) Provide technical assistance to the OIG in support of case investigations;

Assessment and Containment

(1) Notify the CIO immediately after confirmation that a security breach has occurred;

(2) Monitor all Departmental network backbone nodes on a 24 hour basis for network incidents/intrusions;

(3) Ensure that suspected backbone network intrusions are reported to the NITC-SNCC for official documentation;

(4) Receive reports of suspected IT Incidents from the following sources:
   (a) FedCIRC and other intelligence sources
   (b) ISSPM/Agency Representatives
   (c) Cyber Security System Engineers
   (d) Agency Individuals

(5) Review all field incident intelligence, facts surrounding the case and Level of Consequence. In coordination with the Agency Information Systems Security Program Manager/Representative, will make a corporate decision concerning countermeasures. Countermeasures can include blocking some/all system activity or monitoring of the system by Cyber Security engineers;

(6) Issue a "Cease and Desist Order" to bring a system down if the agency does not respond and the problem is not contained in a timely manner (normally 12 hours);

Recovery

(1) Deploy the "Cyber Corps" to augment agencies incident response or to protect departmental information assets, if required;

(2) Review all agency requests for compromised systems/applications to resume normal operations in conjunction with results of Cyber Security system scans. Approve/disapprove system/application/web page return to normal operation within 24 hours of formal agency request;

(3) Be responsible for notifying the CIO with information concerning all Major IT Security Incidents; provide regular updates based on the gravity of threat;

Incident Reporting

(1) Escalate as necessary major IT Incident cases of high magnitude with the OIG;
(2) In cases of illegal/inappropriate activities, refer the case back to the agency for administrative actions against employees/contractors, if the OIG elects not to investigate; and
(3) Assure that this procedure is modified as necessary, disseminated and enforced on behalf of the CIO.

c USDA Departmental ISSPM/Deputy ISSPM will:

General

(1) Serve as the Department POC for collecting and analyzing information on incidents;
(2) Maintain a current centralized listing of all Internet Protocol (IP) Address ranges for all USDA activities;
(3) Maintain a current telephone and E-mail Listing of all agency ISSPM and their alternates;
(4) Maintain contact with internal/external parties and provide whatever assistance is needed to ensure that activities required to resolve an IT Computer Incident are taken;
(5) Report to the Associate CIO for Cyber Security all IT incidents immediately;

Assessment and Containment

(1) Review all USDA IT Intrusions Reports as received (Daily Incident Reports and Reports From Firewalls/Intrusion Detection Systems);
(2) Notify the agency ISSPM or agency representatives of suspected incidents in their environments;
(3) Coordinate with agencies to make an agency decision regarding the incident. Possible decisions include: shut down of system, blocking of external/internal activity, or careful monitoring of affected system;
(4) Notify the Associate CIO for Cyber Security of all major IT Security Incidents/Intrusions and agency responses to each threat on an ongoing basis;
(5) Assign an OCIO Incident Number (OCIO XXXXX) to each case. Report the incident electronically to FedCIRC for review and action. FedCIRC will assign a FedCIRC Incident Number, review the case and provide recommended actions

via E-mail; Forward the FedCIRC information to the agency ISSPM;

(6) Coordinate the deployment of the Cyber Corps when authorized by the Associate CIO for CS;
(7) Advise and assist the agency ISSPM in the assessment and containment actions, as necessary;
(8) Provide a consolidated report on all open agency IT incidents weekly with progress on agency resolutions;
(9) Provide progress reports on all open incidents weekly;
(10) Send an electronic report daily to ISSPMs on penetration exploits that are fast paced; more routine penetration exploits will be reported weekly to the ISSPMs via E-mail;
(11) Maintain a current database of all IT Incidents

Incident Reporting

(1) Assist the agency ISSPM with the incident response and preparation of all IT incident Reports outlined in the Figures of this regulation;
(2) Ensure that incident-handling actions taken are in accordance with established policies and procedures including incident close out;
(3) Provide copies of the latest information on Security Products, Breaches and Alerts to the agency ISSPMs to increase their level of security awareness; and
(4) Provide monthly reports of all IT incidents to the Associate CIO for Cyber Security.

d The OCIO, National Information Technology Center, Systems Network Control Center (NITC-SNCC) will:

Incident Reporting

(1) Provide a Point of Contact for formally reporting IT Computer Incidents, 24 hours a day, seven days per week;
(2) Utilize the Agency Incident Contact List for agency notification of suspected IT intrusions; and
(3) Receive and document suspected IT Computer Incident Reports, regardless of source. Complete the Daily Incident Report for all suspected intrusions and forward the information electronically on an as reported basis to the Departmental ISSPM for further action.

e The Office of the Inspector General will:

Incident Reporting

(1) Provide notification of case disposition electronically to the Associate CIO for Cyber Security. Possible disposition includes: internal investigation, referral to the FBI or no action. Case disposition will be noted in the notification;
(2) Ensure that IT Incidents involving threats are forwarded to the FBI, Violent Crimes Unit for action. Notification will be provided to CS of this action;
(3) Provide accelerated support and investigative assistance to the Associate CIO for Cyber Security on all major IT Incidents Involving a high level of magnitude. Provide case disposition notification within 5 days from receipt of official report to include proposed investigative actions and time frames;
(4) Advise CS of any investigative actions involving routine IT Incidents and on a quarterly basis; supply updates on pending cases, as often as a significant development occurs; and
(5) Provide cyber security intelligence information when received to the Associate CIO for Cyber Security.

f Agency Management and /IT Officials (including agency Senior Management, Line Managers, Senior Information Resources Management Official/CIO/Division Directors/Systems Managers) will:

General

(1) Establish and implement internal tactical procedures for reporting and responding to IT Computer Incidents to augment this regulation;
(2) Ensure procedures include the system shutdown and mitigation actions necessary to safeguard agency systems/information assets. In all cases, the safety of USDA information assets must take priority over system availability;
(3) Respond to requests from the Associate CIO for Cyber Security for administrative action against agency personnel/contractors as a result of unauthorized or illegal IT Incidents;
(4) Assign telecommunications and security personnel to the Cyber Corps as needed;
(5) Ensure that an accurate listing of all IP Addresses assigned to all agency activities is maintained by the ISSPM and updated as changes occur;

Assessment and Containment

(1) Take the appropriate containment actions to provide adequate security in the agency environment; assume the responsibility for final resolution of all IT Computer Incidents;
(2) Collaborate with CS promptly in making the necessary corporate and agency level incident containment decisions;
(3) Ensure that the agency ISSPM is actively engaged in the incident process from the outset; delegating backup personnel to act for the ISSPM in their absence to handle incident responsibilities;
(4) Establish an agency IRT with the necessary skills and knowledge to quickly respond to agency threats; designate an individual to oversee this team and be responsible for the IRT; the agency ISSPM/Staff will be a standing member of this team;
(5) Make certain that system administrators, in collaboration with the agency Information Systems Security Program Managers, rapidly implement the actions required to mitigate or correct any identified incident and perform interim/follow-up activities until the incident is officially closed;
(6) Assure that all respective System Administrators, IT personnel, and agency employees are aware of the requirement to report all suspected computer attacks, virus, threats or suspicious activity to the OCIO, NITC- SNCC. The OCIO Incident Contact List, Figure 3, contains the phone number for this activity;

Recovery

(1) Run scans on affected IP address to ensure the vulnerability is corrected; false positives need to be verified with Cyber Security;
(2) Request approval from the Associate CIO for Cyber Security to return compromised systems/applications to operational status; ensure that compromised systems/applications remain off line and disconnected from the Internet until approval is received.

Damage Analysis and Determination

(1) Ensure that system owners/business managers participate in the IT Incident damage assessment process with regard to determination of the value/sensitivity of information and review/concurrence in the final damage report;
(2) Ensure that a Privacy Assessment is performed;

(3) Determine loss of Program Support of the affected system.

Incident Reporting

(1) Provide oversight in the development and completion of appropriate incident reporting documentation including the formal reports identified in the Figures of this regulation within the required time frames;
(2) Make certain that actions are taken to prevent major IT Incident recurrences, including a formal Action Plan with time frames to cover all Intrusions that cannot be corrected immediately; and
(3) Describe agency's plan for correcting similar devices in the network.

g The agency Information Systems Security Program Managers (ISSPM)/designate will:

General

(1) Be the focal point for the agency in the review, containment and final resolution of all IT Computer Incidents;
(2) Serve as the agency POC for all law enforcement investigations of IT Computer Incidents, including those by the OIG. Promptly report and refer IT Incidents involving employee threats to the OIG for further action. The threatening E-mail (s) should be printed and faxed to the designated OIG office and the Departmental ISSPM. The printed copies will be kept in a locked file cabinet or safe for evidentiary purposes;
(3) Review the Agency Incident Contact List every 30 days to ensure accuracy of the data. Send all changes/updates electronically to CS for further action;
(4) Ensure that all FedCIRC emergency advisories, alerts or notifications are promptly forward to individuals responsible for agency systems; act as an advisor to agency IT managers regarding Security products/solutions based on own knowledge or information received from CS;
(5) Maintain a current and accurate listing of IP Addresses assigned to all agency activities and update as changes occur; this listing will be furnished to the Department ISSPM monthly and updated as changes occur;

Assessment and Containment

(1) Review all agency intelligence reports on IT Incidents from all sources and in coordination with CS promptly make corporate and agency containment decisions to protect USDA information technology assets;

(2) Electronically file a Daily Incident Report, Figure 1, within 24 hours of discovery of an event with CS, Departmental Information Systems Security Program Manager/Deputy; provide required information in this report including IP address, type of information being processed and preliminary incident information;

(3) Begin the rapid coordination of IT Incident assessment, containment, recovery and damage analysis actions for compromised systems/applications/web pages;

(4) Provide immediate notification to the agency IRT of the incident and facts surrounding the case; participate in the overall actions of the team to effectively respond to each intrusion; take an active role in ensuring that IRT members are trained and responsive to major IT Intrusions.

(5) Prepare the IT Incident Report, Figure 2, and include all required general, contact and host information, incident category data, security tools in place, and detailed descriptions of the incident as soon as possible during the assessment and containment process. The final report should also include agency Lessons Learned and the formal Damage Analysis Report. Interim reports using this form will be provided electronically to the Departmental ISSPM/Deputy to provide updated status on each major IT Incident. Each report that is an update should be noted as such at the top. The completed electronic report is due to CS 30 days after discovery of the event and prior to the return of the compromised system/application to normal operation and should be noted as the final report;

(6) In coordination with the respective System Administrator, monitor the compromised system/application if shutdown has not occurred. If the level of consequence escalates, the ISSPM will take further containment actions, including shutdown or rendering the system unavailable to the attacker, to preclude further intrusion or damage. For systems that need to be shutdown, always bring the system to a HALTED state and never REBOOT during shutdown of a compromised system. Examine each affected system to determine what changes occurred, such as the addition of new user identifications or software. Diagnostic testing will be

performed on the compromised system (s) to determine the security status using scanning tools;

Recovery

(1) In concert with the Systems Administrator, ensure that the penetrated system is kept offline and disconnected from the Internet until it has been determined how the intrusion occurred and until the vulnerabilities that allowed the penetration have been corrected or disabled. The ISSPM will make certain that log files are copied to another unaffected system. Reboot of the system will be controlled and done in "single-user mode" only;

(2) In coordination with the Systems Administrator, ensure that vendor's guidelines and instructions for restarting mainframes or clustered minicomputer systems are followed. The original Operating System Software will be utilized that represents a "trusted backup" of the operating system prior to the intrusion. All necessary system patches and authorized application software will then be reloaded. All user accounts and system privileges need to be verified for validity prior to reloading. A scan tool will be run on the system by the agency to ensure that the system is ready for operation and secure. Note all system operating software, patches, authorized applications software and data backup tapes should always be stored in a secure location in the event a system restoration is necessary. System data should be backed up on a routine basis dictated by the value or sensitivity of the information.

(3) Ensure that a proper "chain of custody" is maintained as outlined below to support the government's responsibility to prosecute intruders. Work with the System Administrator to ensure that two backup tapes are created. These tapes will be labeled with the date, time, description of data and signature of the person creating the tape. The ISSPM will maintain these tapes in a safe or locked file cabinet with a signed receipt that the tapes have not been reused. The original tape will be provided to investigating authorities; the second copy will be retained by the ISSPM. It is strongly recommended that a witness be present to document and attest to the events that occurred in the process of protecting evidence.

(4) Upon notification by the respective System Administrator that the system is secure and ready for normal operation, the

ISSPM will advise the CS, Departmental ISSPM of system recovery and request approval to resume normal operation.

Damage Analysis and Determination

(1) In concert with the systems owner or IT business manager, make a determination on the value/sensitivity of the data to the agency mission. Collaboratively develop a damage determination based on an analysis of the incident. This analysis should include the type of products used by the intruder, any apparent File Transfer Protocol (FTP)s of data, and the extent of the intrusion. This information should be used as the basis for a decision on the known potential for damage to the system. The damage determination should also be quantified in terms of loss of system availability, loss of response capability to customer, cost of repairing hardware/software and the hours of personnel associated with repair or restoration of the system;

(2) Perform a Privacy Assessment to determine if privacy data has been compromised.

Incident Reporting

(1) Report all suspected IT Computer Incidents to the NITC-SNCC for formal documentation;

(2) Ensure that all IT Incident Reports are completed and filed in the formats and time frames outlined in the previous Policy Section, Incident Response Forms, Contact Lists and Time Frames; and

(3) Retain all incident report information, evidence tapes and other related materials in a safe or locking file cabinet; act as the official agency repository for all IT Computer Incidents.

h The agency Systems Administrators will:

Assessment and Containment

(1) In coordination with the agency ISSPM, will take actions to effectively assess, contain, and recover from all IT Incidents; examine the compromised system to determine what changes occurred to the system as outlined in the duties of the agency ISSPM. Remove all unknown code and software from the compromised system;

(2) Actively participate, if requested, in the internal Incident Response Team and provide subject matter expert advice in the handling of IT Incidents to the agency ISSPM;

Recovery

(1) Rebuild the compromised system, as outlined in the ISSPM duties above, conduct system scans and notify the agency ISSPM when the system is secure and ready to resume normal operation;
(2) Ensure that all system patches have been applied;
(3) Test the system to determine that vulnerabilities have been corrected or adequately mitigated;

Damage Analysis and Determination

(1) Assist the agency ISSPM in any research or investigation required to determine the extent of any damage done or the impact of the IT incident on the system(s) administered;
(2) Preserve and protect the evidence compiled as a result of the investigation or research;
(3) Ensure that forensic evidence has been maintained; and

Incident Reporting

(1) Report any suspected intrusion to the appropriate IT Manager, agency ISSPM and NITC-SNCC immediately upon learning of the incident.

i All Agency Employees will:

General

(1) Report all suspicious computer related activities immediately when detected on USDA Systems to the responsible System Administrator, agency Information System Security Program Manager or HELP Desk personnel for investigation and determination of whether an incident has occurred or is in process.

- END -

FIGURE 1

DAILY INCIDENT REPORT

THIS FORM IS DUE WITHIN 24 HOURS OF DISCOVERY OF AN IT INCIDENT.

Name of Caller: E-mail Address:
Organization/Agency of Caller:
Phone Number(s) of Caller:
Date/Time of Discovery:

Website or Server Location, if available:

How Caller Obtained Information Being Reported:

Where More Info May be Available (website, another person [Name/Number], another organization [Name/Number]:

Potential Impact, if known:

IP Address:

Date/Time Agency Contact Accomplished:

Other Comments:

DAILY INCIDENT FOLLOW-UP REPORT

Organization/Agency Contacted:
Name of Person Contacted:
Date/Time Contact Was Made:

Type of Message Left: (Direct Contact, Voice Mail, E-mail, Fax)

Description of Message Left:

Additional Comments:

FIGURE 2

IT INCIDENT REPORT FORM

THIS FORM MUST BE COMPLETED WITHIN 30 DAYS OF DISCOVERY OF AN IT INCIDENT.

I. GENERAL INFORMATION [Section I, must be completed entirely]

OCIO Incident Number:_____ Date: _____

Organization Name :_____

FedCIRC Incident Number: _____

Reporting Site Organization Name:_____

Domain Name: _____

Brief Description of the affected organization: (Duties, Responsiblities)

_____

_____

II. CONTACT INFORMATION [* means section/item must be completed]

***** Primary Contact: _____
E-Mail Address: _____
Telephone number:_____
Cell Phone Number:_____ FAX number:_____
Pager number: _____
Home telephone number: _____

Secondary Contact: _____
E-Mail Address: _____
Telephone number:_____
Cell Phone Number:_____ FAX number:_____
Pager number: _____
Home telephone number: _____
Secure communication Channel (yes/no):

ISSPM Name: _____
E-Mail Address: _____
Telephone number:_____
Cell Phone Number:_____ FAX number:_____

Pager number: _____
Home telephone number: _____
Secure communication Channel (yes/no):

Contact from other site(s) involved in this incident

Site name: _____
Contact name: _____
E-Mail address: _____
Phone Number: _____
Pager Number_____
FAX Number: _____
Security communication channel (Yes/NO):

***** Information about other USDA contacts:
USDA Organization:_____
Organization Address: _____
Contact Name: E-Mail Address: _____
Telephone number:_____
FAX number:_____

***** Contact Information about site through which incident occurred:
Site name: _____
Contact name: _____
E-Mail address: _____
Phone Number: _____
Pager Number_____
FAX Number: _____
Security communication channel (Yes/NO):

***** Contact Information about site from which incident began:
Site name: _____
Contact name: _____
E-Mail address: _____
Phone Number: _____
Pager Number_____
FAX Number: _____
Security communication channel (Yes/NO):
Domain Name: _____

Contact Information about USDA ISSPM or OIG contact(s):
Contact name: _____
E-Mail address: _____
Phone Number: _____
Pager Number_____
FAX Number: _____

III. HOST INFORMATION [Section III, must be completed entirely]

Please provide information about all host(s) involved in the incident. Each host shall be listed separately.

Host name: _____
IP Addresses: _____
Vendor hardware: _____
Operating System and version: _____

Security patches applied/installed as currently recommended by the vendor. List version and date of installation. (Please provide on separate sheet of paper.)

Function(s) of the involved host:
_____
Router: _____
Server: _____
Mail Hub: _____
DNS - external or internal: _____

Where on the network is the involved host? - Backbone; subnet:
_____
_____
_____

Nature of the information at risk on the involved host - configuration, proprietary, personnel, financial, Privacy Act.
_____
_____
_____

Time zone of the involved host: _____
Were clocks synchronized? (Yes / No)

Was the host the source or victim of the attack or both:
_____

Was this host compromised as a result of the attack? (Yes / No)
# of users affected _____ Hours system down_____
Estimated $ Loss _____

IV. INCIDENT CATEGORIES

All categories applicable to the incident shall be documented.
Probe(s): _____
Scan(s): _____

Prank: _____
Scam: _____
E-Mail Spoof: _____
E-Mail bombardment: _____
Was this a denial-of-service attack? _____

Break-In:
Intruder gained "root access": (Yes / No)
Intruder installed a Trojan horse program: (Yes / No)
Intruder installed a packet sniffer: (Yes / No)
If Yes:
What was full path name(s) of the sniffer output file(s):
_____

How many sessions did the sniffer log?
(Use "grep –c 'DATA'<filename>" to obtain this information)

In each of following, circle yes or no:

NIS (yellow pages) attack (Yes / No)
NFS attack (Yes / No)
TFTP attack (Yes / No)
FTP attack (Yes / No)
Telnet attack: (Yes / No)
Rlogin or rsh attack (Yes / No)
Cracked password (Yes / No)
Easily-guessable password (Yes / No)
Anonymous FTP abuse (Yes / No)
IP Spoofing (Yes / No)

Product vulnerability Explain:

_____

Misuse of host(s) resources (Yes / No)

V. SECURITY TOOLS [* means section/item must be completed]

* At the time of the Incident, was the organization using any of the following? (Yes / No):

Banner Warning: _____
Network Monitoring Tools: _____
Authentication/Password tools: _____
Service filtering tools: _____

Tools to scan hosts for vulnerabilities: ISS/SATAN

Multipurpose tools: C2 security COPS Tiger (Circle all that apply)
Other tools: lsof cpm smrsh append-only file systems virus scanner(s)
(Circle all that apply)
Were logs being maintained: If so, please describe.

_____
_____
_____

VI. DETAIL INCIDENT DESCRIPTION

Detailed Incident Description: This should be as detailed as possible (especially when writing lesson learned or after the incident follow-up report. Please use separate sheets of paper to address the following:

A. Duration of Incident:
B. How was the incident discovered?
C. Method(s) used by intruders to gain access to host(s):
D. Detailed discussion of vulnerabilities exploited that are not addressed in previous sections:
E. Hidden files/directories:
F. Source of attack (if known):
G. Did system contain classified/sensitive information? What type?
H. Was the information compromised?
I. Was the matter referred to the FBI/law enforcement authorities for further action? If so, to whom?
J. How did/does your organization plan to address the incident?
K. Attach log file:

FIGURE 3

OCIO INCIDENT CONTACT LIST

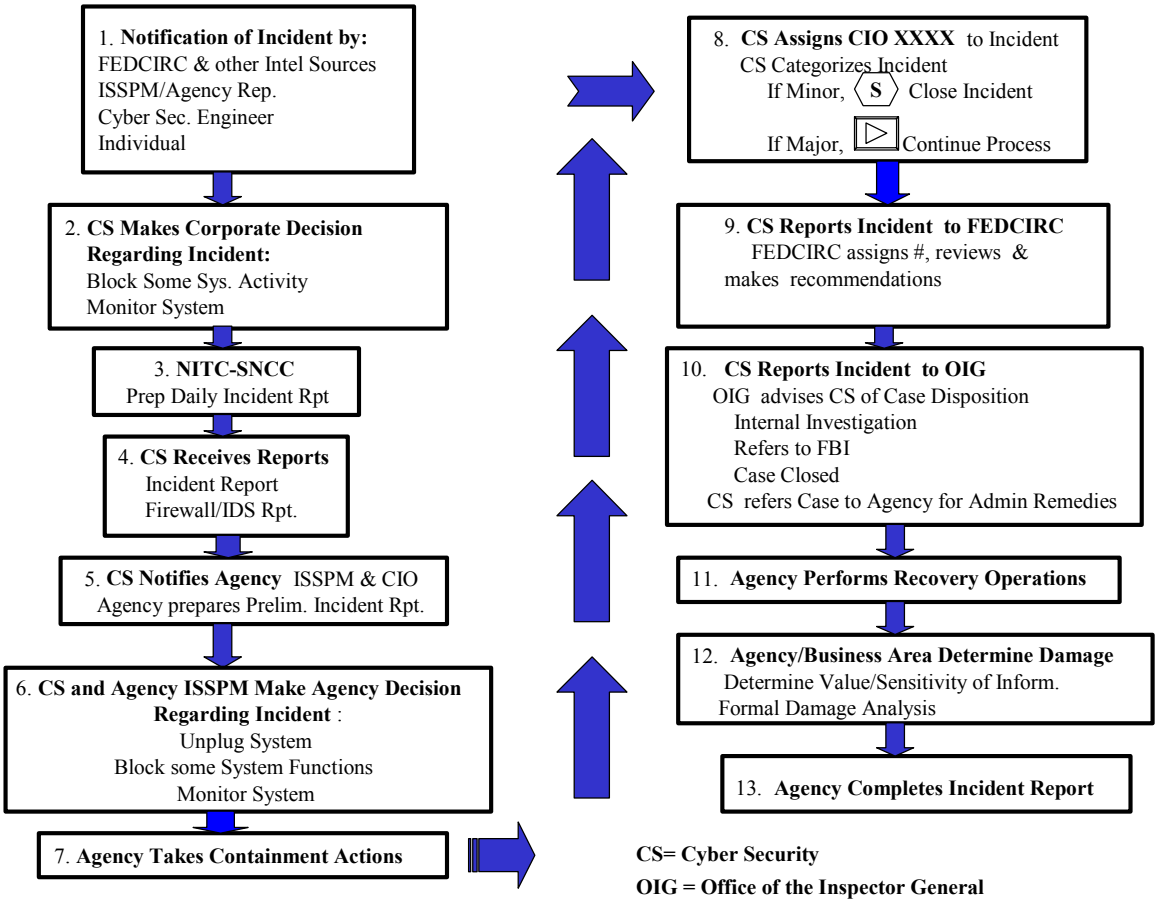
CONTACT PERSON	WORK PHONE	HOME PHONE	PAGER NO.
USDA CIO	202-720-8833		
USDA Deputy CIO	202-720-8833		
USDA Associate CIO	202-690-1361		
USDA ISSPM	202-720-3230		
USDA Deputy ISSPM	202-720-6355		
NITC-SNCC	816-926-6660		
USDA OIG	202-720-6701		
FEDCIRC HOT LINE	412-268-6321		
TOLL Free Number	1-888-282-0870		
FAX Number	1-412-268-6989		
F. B. I.			
Spec. AGENT PETER Vu *	703-762-3168		
Spec. AGENT ATKINS	202-720-8025		

* WASHINGTON FIELD OFFICE REGIONAL COMPUTER CRIME SQUAD

FIGURE 4
AGENCY INCIDENT CONTACT LIST

Agency	Name	Title	Phone Number	E-mail Add.

FIGURE 5 - IT INCIDENT PROCESS 5/3/01



CS= Cyber Security

OIG = Office of the Inspector General